Digital Citizenship Manual (REVISED)

Ivory Robinson

University of West Alabama

09-17-14

**TABLE OF CONTENTS**

**SECTION 1**

**DEFINITION OF DIGITAL CITIZENSHIP 3**

**SECTION 2**

**CLASSROOM RULES FOR CELL PHONES 3**

**SECTION 3**

**SOCIAL NETWORKING AND CYBERBULLYING POLICIES 3-4**

**SECTION 4**

**EMAIL AND INTERNET SAFETY 4-5**

**SECTION 5**

**COPYRIGHT AND PLAGIARISM 6**

**SECTION 6**

**DIGITAL ACCESS 7**

**SECTION 7**

**CLASSROOM COMPUTER RULES 8**

**SECTION 8**

**SUMTER COUNTY ACCEPTABLE TECHNOLOGY USE POLICY 8**

**SUMTER COUNTY PROHIBITED INTERNET CONDUCT 9-11**

**SECTION 9**

**VIDEOS ON DIGITAL CITIZENSHIP 12-13**

**SECTION 12**

**REFERENCES 14**

**What is Digital Citizenship?**

Digital Citizenship is navigating through the digital world responsibly, ethically and safely.

**School and District Policies**

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the Internet are often public in nature. General school rules for behavior and communications apply (See Student Handbook). The Internet is provided for students to conduct research and communicate with others. Access to Internet services will be provided to students who agree to act in a considerate and responsible manner.

**Social Networking**

\*What is Social Networking and how is it beneficial?

Social networking is the grouping of individuals into specific groups, like small rural communities or a neighborhood subdivision, if you will. Although this can be done in person, social networking is most popular online amongst high school and college students. This is beneficial because it allows millions of people around the world to meet and interact with each other without physically being near each other. It allows people with common interests (music, sports team, fashion, etc.) to gather in a community via online and socialize.

**Cyberbullying**

Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.



\*What are the effects of cyberbullying and how can it be prevented?

Cyberbullying symptoms include sadness, irregular sleeping and eating patterns, a loss of interest in social activities and anxiety just to name a few. Sadly, it can even lead to suicide. Cyberbullying can be prevented by these steps:

1. Personalize your settings on your social media page. Make sure only people you know personally can see and interact with your profile.

2. Be mindful of what you place online. Photos, comments, etc. that may be embarrassing to you should not be uploaded to any of your social networking profiles. Don’t give bullies ammunition to use against you.

3. Go to a search engine and research your name. Make sure you don’t still have an active account with any old social networking sites that you may rarely or no longer use. There may be something personal displayed that you don’t want anyone else to know.

**Email and Internet Safety**

\*What is an email and how is it beneficial?

An email is a message distributed by electronic means from one computer user to one or more recipients via a network. Emails are beneficial because it allows instant mass communication between people. Be cautious of spam (unwanted emails that people send in order to try to get personal information from you in order to hack your identity. If it sounds too good to be true, it likely is).

\*What is the internet?

The internet is a vast computer network linking smaller computer networks worldwide. The Internet includes commercial, educational, governmental, and other networks, all of which use the same set of communications protocols.

**Internet Safety: Tips on protecting yourself on the web**

1. Use strong and unique passwords when creating accounts to ensure that your information is not easily accessible to hackers.

2. Purchase and download a known and effective antivirus program to protect your computer from viruses such as Trojans, worms and spyware. Viruses can potentially destroy your computer or make them expensive to repair once the virus has set in.

3. Avoid scams via websites and emails. Anytime someone offers you something for money in return, it typically is some kind of scam. If it sounds too good to be true, it usually is.



4. For those with children who use the internet, it is necessary to purchase program blockers to block access to inappropriate and adult-oriented websites.

5. It is very important that parents monitor their children’s use of the internet to ensure there is no inappropriate interaction with strangers.

6. For family households with internet access, put the family computer in a high-traffic are of your home. This makes monitoring much easier.

**Copyright & Plagiarism**

\*What is a copyright?

A copy right is the exclusive legal right, given to an originator or an assignee to print, publish, perform, film, or record literary, artistic, or musical material, and to authorize others to do the same.

\*What is plagiarism?

Plagiarism is the practice of taking someone else's work or ideas and passing them off as one's own. (Synonyms: copying, infringement of copyright, piracy, theft and stealing).

**What you need to know about plagiarism and the internet:**

The most common practice of plagiarism on the internet is piracy. This includes, but is not limited to, the illegal downloading of movies, music, games, software, etc. Piracy is illegal and if convicted of this crime, one may endure hefty fines or even a jail sentence. In the end, it’s just not worth it.



**Copyright (Sumter County)**

Unauthorized use of copyrighted material is prohibited. All copyrighted material must be properly cited using standard citation information. Giving credit (web address or active link) to a company or individual (celebrity, for instance) that has created text, a graphic, etc. for a school page may be allowed, assuming the site is not blocked by the web filtering hardware and software.

**Digital Access**

The students’ time to use technology in the classroom should be based on the current curriculum and whether or not technology can be useful. If the computer space is limited, students should be given times slots throughout the week based on the alphabetical order of their last names. Nevertheless, the rules/tips are effective in either situation:

Tip 1: So that you don¹t have to reinvent the wheel each year and so that students can use the computer center independently, write directions for computer activities on index cards or poster board and laminate them.

Tip 2: Try to create activities that correlate to your current studies - you may want to check your teacher's guides for suggestions of related computer activities. Once you come up with a great idea, make a note in your subject area guide so that you'll remember to use it when you come to that unit again next year.

Tip 3: When it comes to activities for your computer center, start with lessons that can be completed in one session. It helps to give all students a chance to have success with several simple computer assignments before trying their hand at a long-term project.

Tip 4: Before assigning an activity try completing the assignment yourself, or even better, find a student to test the activity for you. (Volunteers for this job are never hard to find in my room!) This will let you know if the activity can be completed in the time you've allotted and if your directions are clear.

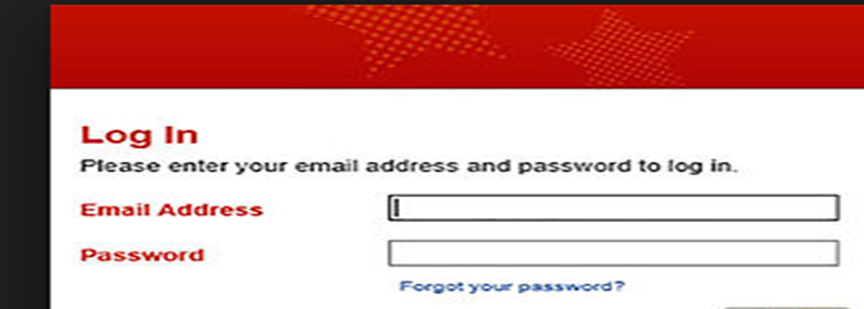
Tip 5: Select a student to be the "Computer Expert" each week. Allow this student to complete the assignment first and then answer any questions that may arise while other students work through the activity. This helps free you from the role of task monitor while allowing your students to become mentors for one another.

Tip 6: Agree on a signal that students can use if they need help while working on a task. My favorite is to place a brightly colored plastic cup next to each computer. When students need help, they place their cup on top of their computer as a signal for assistance. Once they've gotten help, the cup is placed beside their computer again.

**Classroom Computer Rules**

In classrooms, there may be limited access to computers, so students will have to take turns using them. The key to this is making sure that each student has a different login profile, so that you may monitor each student web access. Just as you have to monitor student’s technology use on their cell phones in class, you have to do the same for desktops or laptops. Schools systems usually distribute code of conduct books that give detail rules about computer usage followed by signed agreement page. Students should also know that these computers are school property and should be used with great care. Any student that doesn’t comply with these rules should be subject to loss of computer usage. Three general tips teachers can go by t along with those rules outline schools are these.

1. Keep student’s profiles check for nuisance activity.



2. Make sure every student is aware that the computers are a privilege and not a right.

3. Keep yourself in tune with the changes in technology.

**Acceptable Technology Use Policy (Sumter County School District)**

Any student who utilizes the computer lab(s) or any computer equipment at the school must be aware of certain policies for use of the equipment and/or facilities. Procedures are in place for the protection of students and equipment. Students will be held accountable for any violation of the following policies (as would be the case for any classroom disciplinary matter). A student and his/her parents will be responsible for damages and will be liable for costs incurred for service or repair.  Students are only allowed to utilize the computers and network to retrieve information and run specific software applications as directed by their teacher. Students are not permitted to explore the configuration of the computer, operating system or network, run programs not on the menu, or attempt to do anything they are not specifically authorized to do.

Students are responsible for ensuring that any diskettes, CDs, memory sticks, USB flash drives, or other forms of storage media that they bring in from outside the school are virus free and do not contain any unauthorized or inappropriate files. Students may not bring personal computers or hand-held computing devices and connect them to the school network or Internet connection (including connecting to wireless access points).

**Prohibited Internet Conduct (Sumter County)**

**Examples of prohibited conduct include but are not limited to the following:**

A. Accessing, sending, creating or posting materials or communications that are:

1. Damaging to another person’s reputation;

2. Abusive;

3. Obscene;

4. Sexually oriented;

5. Threatening or demeaning to another person;

6. Contrary to the school’s policy on harassment;

7. Harassing; or

8. Illegal

B. Using the network for financial gain or advertising.

C. Posting or plagiarizing work created by another person without their consent.

D. Posting anonymous or forging electronic mail messages.

E. Attempting to read, alter, delete, or copy the electronic mail messages of other system users.

F. Giving out personal information such as phone numbers, addresses, driver’s license or social

security numbers, bankcard or checking account information.

G. Using the school’s computer hardware or network for any illegal activity such as copying or

downloading copyrighted software, music or images, or violation of copyright laws.

H. Downloading, installing, or using games, music files, public domain, shareware or any other

unauthorized program on any school’s computer or computer system.

I. Purposely bringing on premises or infecting any school computer or network with a Virus, Trojan,

or program designed to damage, alter, destroy or provide access to unauthorized data or

information.

J. Gaining access or attempting to access unauthorized or restricted network resources or the data

and documents of another person.

K. Using or attempting to use the password or account of another person or utilizing a computer

while logged on under another user’s account.

L. Using the school’s computers or network while access privileges have been suspended.

M. Using the school’s computer hardware, network, or Internet link in a manner that is inconsistent

with a teacher’s directions and generally accepted network etiquette.

N. Altering or attempting to alter the configuration of a computer, network electronics, the operating

system, or any of the software.

O. Attempting to vandalize, disconnect or disassemble any network or computer component.

P. Utilizing the computers and network to retrieve information or run software applications not

assigned by their teacher or inconsistent with school policy.

Q. Providing another student with user account information or passwords.

R. Connecting to or installing any computer hardware, components, or software which are not

school system property to or in the district’s technology resources without prior approval of the

district technology supervisory personnel.

S. Bringing on premises any disk or storage device that contains a software application or utility that

could be used to alter the configuration of the operating system or network equipment, scan or

probe the network, or provide access to unauthorized areas or data.

T. Downloading or accessing via e-mail or file sharing, any software or programs not specifically

authorized by Technology personnel.

U. Bypassing or attempting to circumvent network security, virus protection, network filtering, or

policies.

V. Possessing or accessing information on school property relating to “Hacking,” or altering, or

bypassing network security or policies.

W. Participating on message boards without teacher direction, or in live chat using but not limited to

AIM, Yahoo, or MSN Messenger.

X. Students should follow the guidelines below when performing Internet searches.



**Videos on Digital Citizenship**

****

<http://www.youtube.com/watch?v=oCkTmZ0bF5Q>

****

<http://www.youtube.com/watch?v=erJ0T9k5aHo>

****

<http://www.youtube.com/watch?v=FdEXijFXfD8>

**References**

CyberWise 1. (2011, June 26). What is Digital Citizenship? Retrieved from http://www.youtube.com/watch?v=oCkTmZ0bF5Q.

Dunn, Jeff. (2013, November 2). 10 Important Rules For Your Schools Computer Lab. Edudemic.com. Retrieved from http://www.edudemic.com/school-computer-lab-rules/. Iclevedon. (2013, May 17). Digital Citizenship- THINK! Retrieved from http://www.youtube.com/watch?v=erJ0T9k5aHo.

Zhang, Xin. (2012, January 11). Be a Digital Citizen. Retrieved from <http://www.youtube.com/watch?v=FdEXijFXfD8>.

Sumter County School District. (2014). Procedures for Internet License. Retrieved from http://scms.sumterschools.org/Common/SchoolArea/HandbookPrint.asp?PolicyID=43962